IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 10/670,298
Filing Date 09/26/2003
Inventorship ..... Klaes
Group Art Unit 2135
Examiner ..... SHAN, April Ying
Attorney's Docket No. ER1-0014US
Title: SECURITY MONITORING AND INTRUSION DETECTION SYSTEM

APPEAL BRIEF

To: MS: Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

From: Tim R. Wyckoff
Customer No. 29150
Lee & Hayes PLLC
421 W Riverside Avenue, Suite 500
Spokane, WA 99201

INTRODUCTORY COMMENTS

Pursuant to 37 C.F.R. § 41.37, Appellant hereby submits an Appeal Brief for Application Serial No. 10/670,298 filed September 26, 2003. A Notice of Appeal was filed on December 10, 2007. Accordingly, Appellant appeals to the Board of Patent Appeals and Interferences (hereinafter "Board") seeking review of the Office's rejections.

TABLE OF CONTENTS

(i) Real Party in Interest

The real party in interest is the Swiss Reinsurance Corporation, the assignee of all right and title to the subject invention.

(ii) Related Appeals and Interferences

Appellant is not aware of any other appeals or interferences which will directly affect, be directly affected by, or otherwise have a bearing on the Board's decision to this pending Appeal.

(iii) Status of Claims

Allowed Claims: No claims have been allowed.

Canceled Claims: No claims have been canceled.

Originally Presented Claims: Claims 1-30 were originally presented when this Application was filed.

Pending Claims: Claims 1-30 stand rejected and are pending in this Application as set forth in the Claims Appendix on page 17.

Appealed Claims: All of the pending claims are subject to this Appeal. Claims 1-30 are rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Claims 12-21 are rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement. Claims 1-21 are rejected under 35 U.S.C. § 101 because it is asserted that the claims are directed to non-statutory subject matter. Claims 1-7, 9-17, 19-28 and 30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Khanolkar et al., U.S. Patent No. 7,127,743 (hereinafter "Khanolkar"). Claims 8, 18 and 29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over

Khanolkar in view of "Admitted prior art" (hereinafter "APA"). The indicated rejections are set forth in the Final Office Action dated August 8, 2007.

(iv) Status of Amendments

An Amendment has not been filed subsequent to the Final Office Action dated August 8, 2007.

(v) Summary of Claimed Subject Matter

The following is a concise explanation of each independent claim 1, 12 and 22 and dependent claim 9 involved in the Appeal and includes, where appropriate, references to the specification (as filed) by page, paragraph and line number, and to the drawings. The claims are not to be limited solely to the elements identified by the reference characters and other related description.

Claim 1 recites a computer-implemented monitoring/intrusion detection system, comprising: a central loghost (*page 5, paragraph [0015], line 13; Figs. 1-3; central loghost 100*), at least one proxy loghost (*page 5, paragraph [0015], line 11; Figs. 1-3; proxy loghost 160*) remote (*page 7, paragraph [0024], line 5; Fig. 1; proxy loghost 160 shown remote*) from the central loghost (*page 5, paragraph [0015], line 13; Figs. 1-3; central loghost 100*) and in communication with the central loghost over a network (*page 5, paragraph [0015], line 10; Fig. 1; network 150*); and at least one monitoring station (*page 9, paragraph [0028], line 1; Fig. 3; alarming module 310*), wherein the proxy loghost receives a plurality of log files (*See e.g., pages 4 & 5, paragraphs [0015] & [0015]*) from a plurality of resources (*page 4, paragraph [0015], line 1; Fig. 1; resources 170*) operating on the network, analyzes the log files for at least one of unexpected volume,

unexpected patterns, or unexpected types of log files (*See e.g., page 7, paragraph [0022]*), and generates events (*See e.g., pages 7 & 8, paragraphs [0025] & [0026]*) in view of such analysis, wherein the central loghost is operable to receive the events generated by the proxy loghost through the network and generate an alert (*See e.g., page 8, paragraph [0027]*) upon an analysis of the events, and wherein the monitoring station is caused to issue an alarm when the alert (*page 9, paragraph [0029], lines 11-12; Figs. 3 & 4; "alarm is 'sounded'"*) is generated.

Claim 9 which depends from claim 1 recites that the log files are archived on the proxy loghost (*See e.g., pages 5 & 6, paragraphs [0018]*) and the events are archived (*page 6, paragraph [0019], line 5; Fig. 1; disk 200*) on the central loghost.

Claim 12 recites a computer-implemented system for detecting intrusion into a secure network, comprising: a plurality of proxy loghosts (*page 5, paragraph [0015], line 11; Figs. 1-3; proxy loghost 160*), each proxy loghost collecting log files (*See e.g., pages 4 & 5, paragraphs [0015] & [0015]*) that are generated by resources in a portion of the secure network, the plurality of loghosts generating events (*See e.g., pages 7 & 8, paragraphs [0025] & [0026]*) in response to the log files collected; and a central loghost (*page 5, paragraph [0015], line 13; Figs. 1-3; central loghost 100*) remote (*page 7, paragraph [0024], line 5; Fig. 1; proxy loghost 160 shown remote*) from the plurality of proxy loghosts and in communication with the plurality of proxy loghosts over a network (*page 5, paragraph [0015], line 10; Fig. 1; network 150*), the central loghost receiving the log files themselves and the events from the plurality of proxy loghosts, the central loghost analyzing the log files and the events to determine the necessity of generating an alert (*See e.g., page 8, paragraph*

[0027]]) and an associated alarm (*page 9, paragraph [0029], lines 11-12; Figs. 3 & 4; "alarm is 'sounded'"*) to notify a security manager (*See e.g., page 6, paragraph [0018]*) of a possible intrusion incident.

Claim 22 recites a method of monitoring a network, comprising: receiving a plurality of log messages at a proxy loghost (*page 9, paragraph [0029], lines 1-2; Fig. 4; Block 410*); analyzing the log messages and determining whether, in the log files, there exists any anomalies or unusual patterns (*page 9, paragraph [0029], lines 3-4; Fig. 4; Block 420*); generating an event in response to the anomalies or unusual patterns and forwarding the event over a network from the proxy loghost to a remote central loghost (*page 9, paragraph [0029], lines 4-8; Fig. 4; Block 430*); monitoring the events at the central loghost and generating an alert in accordance with predetermined event analysis (*page 9, paragraph [0029], lines 8-13; Fig. 4; Block 450*); and generating an alarm communication in coordination with the alert, the alarm being indicative of an unwanted incident in the network (*page 9, paragraph [0029], lines 8-13; Fig. 4; Block 460*).

(vi) Grounds of Rejection to be Reviewed on Appeal

Claim Rejections Under 35 U.S.C. § 112

Claims 1-30 are rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.

Claims 12-21 are rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement.

Claim Rejection Under 35 U.S.C. § 101

Claims 1-21 are rejected under 35 U.S.C. § 101 because it is asserted that the claims are directed to non-statutory subject matter.

Claim Rejection Under 35 U.S.C. § 103

Claims 1-7, 9-17, 19-28 and 30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Khanolkar.

Claims 8, 18 and 29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Khanolkar in view of "Admitted prior art" (hereinafter "APA").

(vii) Argument

(A) Claims 1-30 fully conform with the 35 U.S.C. § 112, first paragraph written description requirement

Independent claims 1, 12 and 22

Each of the rejected independent **claims 1, 12 and 22** recites that the central and proxy loghosts are "remote" from each other. The Office states Appellant's disclosure discloses that "both proxy and central loghosts" are "independent modules that can run on the same system," and therefore, the central and proxy loghosts are not remote from each other. (*See page 2, point 5, Office Action of August 2008.*) The Appellant respectfully submits the Office's understanding of the term "remote" is incorrect and that there is indeed support for the use of "remote" in the claims.

As those of ordinary skill in the computer related arts appreciate, the word "remote" does not necessarily describe or denote great distance between a plurality of elements. To the contrary, the word remote may simply mean that two or more elements, entities, or elements are spatially separate, but a great amount of separation is not required. Therefore, the Office's argument that "two computers

under the same system" and in very "close proximity" are not "remote" is not correct. Moreover, Wikipedia (wikipedia.org) defines "remote" computer as "a computer to which a user does not have physical access, but which he or she can access/manipulate via some kind of network from a local computer (one which the user does have physical access to)." As is shown in Fig. 1 of the instant Application, the central loghost 100 and the proxy loghost 160 are separated by the network 150. Thus, the central loghost 100 and the proxy loghost 160 are remote from each other. Appellant respectfully submits that this illustration and the disclosure of the instant Application, coupled with the definition from Wikipedia, further support the use of "remote" in the claims.

Further to the above, the instant Application has explicit disclosure that provides support for describing the central loghost and the proxy loghost as being remote from each other. For example, *paragraph [0024], line 5*, discloses "the remote proxy loghost."

The Office maintains the inclusion in **claim 12** of both "a plurality of proxy loghosts" and "a central loghost," where the "central loghost" receives "the log files themselves and the events from the plurality of proxy loghosts, the central loghost analyzing the log files and the events…" is not supported by the instant Application. The Appellant respectfully disagrees for the following reasons.

The proxy and central loghosts are independent modules (*See paragraph [0017], lines 1-2*), and stored log files and event files can be remotely accessed on proxy loghosts 160 and central loghosts 100 using https (*See paragraph [0018], lines 1-3*). Therefore, both loghosts 160 and 100 may include log files and event files.

The proxy and central loghosts also include common software modules. (*See paragraph [0019], lines 1-2.*) For example, both loghosts 160 and 100 include a "logsurf" module that is a real time log file analysis module that generates events and alerts. (*See paragraph [0021], lines 1-8; see also Fig. 2.*) Therefore, both loghosts 160 and 100 may generate events and alerts. In addition, both loghosts 160 and 100 may include a "syslog-ng" module (*See paragraph [0020], lines 1-7; see also Fig. 2.*) The syslog-ng module operating on proxy log hosts 160 is somewhat different from the syslog-ng module operating on central log host 100 in that the syslog-ng operating on proxy loghosts 160 is configured to receive log files and then forward event files to central loghost 100. (*See paragraph [0020], lines 1-7; see also Fig. 2.*) The syslog-ng on the central loghost 100 does not generally forward event files. Nonetheless, both syslog-ng modules may receive log files.

The above shows that both the proxy loghost 160 and the central loghost 100 may be part of a common enterprise, and that the central log host 100 is capable of "analyzing the log files and the events," as is claimed, even when a proxy loghost 160 is implemented as part of the system. Therefore, at least the disputed subject matter of claim 12 is fully supported by the disclosure of the instant Application.

Appellant does not dispute that it "some cases" it "may" be beneficial to eliminate the use of proxy loghosts when an enterprise is sufficiently small. (*See paragraph [0031].*), as a small enterprise likely does not generate a sufficient volume of log files necessitating the use of the proxy loghosts. That is, the central loghost would likely provide sufficient log file handling for such an environment.

However, this does not preclude the system claimed by claim 12, for example, when the enterprise is other than "sufficiently small."

For the reasons given above, the Board is asked to reconsider and withdraw of the 35 U.S.C. § 112, first paragraph, rejections.

(B) Claims 12-21 fully conform with the 35 U.S.C. § 112, first paragraph enablement requirement

Independent claim 12

The Office maintains the inclusion in **claim 12** of both "a plurality of proxy loghosts" and "a central loghost," where the "central loghost" receives "the log files themselves and the events from the plurality of proxy loghosts, the central loghost analyzing the log files and the events…" is not supported by the instant Application and thus the enablement requirement is not met. The Appellant respectfully disagrees for the following reasons.

The proxy and central loghosts are independent modules (*See paragraph [0017], lines 1-2*), and stored log files and event files can be remotely accessed on proxy loghosts 160 and central loghosts 100 using https (*See paragraph [0018], lines 1-3*). Therefore, both loghosts 160 and 100 may include log files and event files.

The proxy and central loghosts also include common software modules. (*See paragraph [0019], lines 1-2.*) For example, both loghosts 160 and 100 include a "logsurf" module that is a real time log file analysis module that generates events and alerts. (*See paragraph [0021], lines 1-8; see also Fig. 2.*) Therefore, both loghosts 160 and 100 may generate events and alerts. In addition,

both loghosts 160 and 100 may include a "syslog-ng" module (*See paragraph [0020], lines 1-7; see also Fig. 2.*) The syslog-ng module operating on proxy log hosts 160 is somewhat different from the syslog-ng module operating on central log host 100 in that the syslog-ng operating on proxy loghosts 160 is configured to receive log files and then forward event files to central loghost 100. (*See paragraph [0020], lines 1-7; see also Fig. 2.*) The syslog-ng on the central loghost 100 does not generally forward event files. Nonetheless, both syslog-ng modules may receive log files.

The above shows that both the proxy loghost 160 and the central loghost 100 may be part of a common enterprise, and that the central log host 100 is capable of "analyzing the log files and the events," as is claimed, even when a proxy loghost 160 is implemented as part of the system. Therefore, at least the disputed subject matter of claim 12 is fully enabled by the disclosure of the instant Application.

Appellant does not dispute that it "some cases" it "may" be beneficial to eliminate the use of proxy loghosts when an enterprise is sufficiently small. (*See paragraph [0031]*.), as a small enterprise likely does not generate a sufficient volume of log files necessitating the use of the proxy loghosts. That is, the central loghost would likely provide sufficient log file handling for such an environment. However, this does not preclude the system claimed by claim 12, for example, when the enterprise is other than "sufficiently small."

For the reasons given above, the Board is asked to reconsider and withdraw of the 35 U.S.C. § 112, first paragraph, rejection.

(C) Claims 1-12 recite statutory subject matter, as required under 35 U.S.C. § 101

Independent claims 1 and 12

The Office maintains the recitation in claims 1 and 12 "would be reasonably interpreted by one of ordinary skill in the art as software, per se." Appellant respectfully disagrees for the following reasons.

Claim 1 recites "a plurality of resources operating on the network" and claim 12 recites a central loghost in communication with a plurality of loghosts "over a network" Appellant respectfully submits, in consideration of the foregoing language alone, that one of ordinary skill in the art would not conclude that the rejected claims are directed solely to software. In particular, those of ordinary skill in the computer art readily understand networks generally comprise various hardware components (e.g., computers and routers), not software alone as suggested by the Office. The Appellant's own disclosure makes this point. (*See e.g., paragraph [0015].*)

Moreover, Appellant previously amended the claims 1 and 12 to include the recitation "computer-implemented system." The Office has refused to give any weight to the added subject matter when determining whether the claims recite statutory subject matter. However, such an approach is inconsistent with established law. In particular, a "computer-implemented system" is clearly a physical thing, and 35 U.S.C. § 101 statutory subject matter includes "new and useful" machines.

Further, the Office has recognized that such subject matter (e.g., methods embodied on computer-readable media) in the preamble renders process or method

claims as being at the very least statutory subject matter under 35 U.S.C. § 101. Therefore, the rejected claims require the same recognition.

For the reasons given above, the Board is asked to reconsider and withdraw of the 35 U.S.C. § 101 rejection.

(D) Claims 1-7, 9-17, 19-28 and 30 are allowable because Khanolkar does not suggest the subject matter of these claims

Independent claims 1, 12 and 22 & dependent claim 9

Each of the rejected independent **claims 1, 12 and 22** recites that the central and proxy loghosts are "remote" from each other. As discussed earlier herein, and as is shown in Fig. 1 of the instant Application, the central loghost 100 and the proxy loghost 160 are separated by the network 150. Thus, the central loghost 100 and the proxy loghost 160 are remote from each other. Khanolkar does not suggest this remote configuration.

Khanolkar describes event parsers 54 and an event manager 55 that are part of the *same* system 10 and also part of the *same* subsystem 50. (*See Khanolkar, col. 3, lines 49-58; Fig. 2.*) Certainly, the event parsers 54 and the event manager 55 are not separated by a network. Therefore, the parsers 54 and the event manager 55 are not remote from each other.

Further to the above, **claim 12** recites that the central loghost receives and analyzes log files and events. Khanolkar fails to suggest a central loghost that receives log files and events, and instead only discloses the event manager 55 as receiving event objects, not log files as claimed.

Regarding **claim 9**, the recitation of this claim provides for the separate archival of log files and events. In particular, the archiving of log files on the proxy loghost and the archiving of events on the central loghost, and where the two loghosts are remote from each other (see claim 1). Such a storage arrangement is not suggested by Khanolkar. In particular, Khanolkar suggests event parsers 54 and the event manager 55 as part of the same event handling subsystem 50 and suggests a database 58 as storing only event objects (not log data). (*See Khanolkar col. 7, lines 10-12 & lines 23-36.*)

Those claims not discussed in particular in the foregoing, are at least allowable due to their dependence upon one of the independent claims discussed hereinabove.

For the reasons given above, Khanolkar does not suggest the subject matter of the rejected claims. Hence, for at least this reason, these claims are allowable.

(E) Claims 8, 18 and 29 are allowable because Khanolkar in view APA does not suggest the subject matter of these claims

At the very least, claims 8, 18 and 29 are allowable due to their dependence upon an allowable independent claim. Moreover, the APA does not remedy the deficiencies discussed herein in connection with Khanolkar. Hence, for at least this reason, these claims are allowable.

Conclusion

Claims 1-30 are in condition for allowance. Appellant respectfully requests reconsideration and withdrawal of the rejections and prompt allowance of the subject application.

Respectfully Submitted,

Lee & Hayes, PLLC

Date: March 12, 2008

By: /Tim R. Wyckoff/
Tim R. Wyckoff
Attorney at Law
Reg. No. 46,175

(viii) Claims Appendix

1. **(Previously Amended)** A computer-implemented monitoring/intrusion detection system, comprising:

a central loghost,

at least one proxy loghost remote from the central loghost and in communication with the central loghost over a network; and

at least one monitoring station,

wherein the proxy loghost receives a plurality of log files from a plurality of resources operating on the network, analyzes the log files for at least one of unexpected volume, unexpected patterns, or unexpected types of log files, and generates events in view of such analysis,

wherein the central loghost is operable to receive the events generated by the proxy loghost through the network and generate an alert upon an analysis of the events, and

wherein the monitoring station is caused to issue an alarm when the alert is generated.

2. **(Original)** The system of claim 1, wherein the central loghost comprises a plurality modules operating in a Unix environment.

3. **(Original)** The system of claim 1, further comprising a plurality of proxy loghosts, each one of the plurality being in communication with the central loghost.

4. **(Original)** The system of claim 1, wherein the resources comprise at least one of an operating system, application, firewall, router, switch and loadbalancer.

5. **(Original)** The system of claim 1, wherein a plurality of events is required to cause the generation of an alert.

6. **(Original)** The system of claim 1, wherein security management has access to both the proxy loghost and the central loghost.

7. **(Original)** The system of claim 1, wherein the log files are received from a network-based intrusion detection system.

8. **(Original)** The system of claim 1, wherein the log files are received from a host-based intrusion detection system.

9. **(Original)** The system of claim 1, wherein the log files are archived on the proxy loghost and the events are archived on the central loghost.

10. **(Original)** The system of claim 1, further comprising software adapters to convert one format of a log file to another format.

11. **(Original)** The system of claim 1, further comprising a module for visualizing the log files received at the proxy loghost.

12. **(Previously Amended)** A computer-implemented system for detecting intrusion into a secure network, comprising:

a plurality of proxy loghosts, each proxy loghost collecting log files that are generated by resources in a portion of the secure network, the plurality of loghosts generating events in response to the log files collected; and

a central loghost remote from the plurality of proxy loghosts and in communication with the plurality of proxy loghosts over a network, the central loghost receiving the log files themselves and the events from the plurality of proxy loghosts, the central loghost analyzing the log files and the events to determine the necessity of generating an alert and an associated alarm to notify a security manager of a possible intrusion incident.

13. **(Original)** The system of claim 12, wherein the central loghost comprises a plurality modules operating in a Unix environment.

14. **(Original)** The system of claim 12, wherein the resources comprise at least one of an operating system, application, firewall, router, switch and loadbalancer.

15. **(Original)** The system of claim 12, wherein a plurality of events is required to cause the generation of an alert.

16. **(Original)** The system of claim 12, wherein security management has access to both the plurality of proxy loghosts and the central loghost.

17. **(Original)** The system of claim 12, wherein the log files are received from a network-based intrusion detection system.

18. **(Original)** The system of claim 12, wherein the log files are received from a host-based intrusion detection system.

19. **(Original)** The system of claim 1, wherein the log files are archived on the plurality of proxy loghosts and events are archived on the central loghost.

20. **(Original)** The system of claim 12, further comprising software adapters to convert one format of a log file to another format.

21. **(Original)** The system of claim 12, further comprising a module for visualizing the log files received at the proxy loghost.

22. **(Previously Amended)** A method of monitoring a network, comprising:

receiving a plurality of log messages at a proxy loghost;

analyzing the log messages and determining whether, in the log files, there exists any anomalies or unusual patterns;

generating an event in response to the anomalies or unusual patterns and forwarding the event over a network from the proxy loghost to a remote central loghost;

monitoring the events at the central loghost and generating an alert in accordance with predetermined event analysis; and

generating an alarm communication in coordination with the alert, the alarm being indicative of an unwanted incident in the network.

23. **(Original)** The method of claim 22, wherein the central loghost comprises a plurality modules operating in a Unix environment.

24. **(Original)** The method of claim 22, wherein a plurality of proxy loghosts receive log files.

25. **(Original)** The method of claim 22, wherein the log files are received from resources comprising at least one of an operating system, application, firewall, router, switch and loadbalancer.

26. **(Original)** The method of claim 22, further comprising generating the alert only after a plurality events are received.

27. **(Original)** The method of claim 22, further comprising remotely accessing, from a single location, both the proxy loghost and the central loghost.

28. **(Original)** The method of claim 22, wherein the log files are received from a network-based intrusion detection system.

29. **(Original)** The method of claim 22, wherein the log files are received from a host-based intrusion detection system.

30. **(Original)** The method of claim 22, further comprising archiving the log files on the proxy loghost and archiving the event on the central loghost.

(ix) Evidence Appendix

None.

(x) Related Proceedings Appendix

None.